Reinforcing supply chain security through organizational and cultural tools within the intermodal rail and road industry

Cigolini, R., Pero, M. and Sianesi, A.

Please cite this paper as:

Cigolini, R., Pero, M., & Sianesi, A. (2016). Reinforcing supply chain security through organizational and cultural tools within the intermodal rail and road industry. The International Journal of Logistics Management. 27(3), pp. 816-836

Link: https://www.emerald.com/insight/content/doi/10.1108/IJLM-02-2014-0023/full/html

Reinforcing supply chain security through organizational and cultural tools within the intermodal rail and road industry

Abstract

Purpose: This paper outlines the role of organizational and cultural tools to increase supply chain security within the intermodal rail and road industry. Three main research questions are set, regarding: (i) what organizational and cultural tools are used by companies within the intermodal rail and road industry, (ii) how these tools impact on security performance and (iii) what environmental factors trigger the use of each tool.

Design/methodology/approach: Thirteen companies within the intermodal rail and road industry have been studied in detail through in-depth case studies.

Findings: Results suggest that organizational and cultural tools impact positively on supply chian security, by reducing collusion and both operative and planning mistakes. In particular, such tools mitigate the effect of lack of cooperation and communication between partners and of inadequate partners.

Practical implications: Results point out that the ability of organizational and cultural tools to increase supply chain security has not been fully exploited yet. Tools to mitigate the negative effects on security of inadequacy of partners are not popular or they are not considered as powerful enough, despite it has been highlighted as the most relevant causal factor of lack of security.

Originality/value: This paper introduces a thorough overview of the effects of cultural and organizational tools on supply chain security and a detailed study of these tools in the area of intermodal rail-and-road transport.

Keywords

Supply chain, cultural tools, security, rail and road.

1. Introduction

Supply Chain (SC) security is the application of policies, procedures and technologies to protect SCs from theft, damages or terrorism (Closs and McGarrell 2004, Bakshi and Gans 2010). SC security encompasses different areas of interests ranging from the security of SC assets (Closs and McGarrell 2004) to the security of physical, information-related and money flows (Veenestra 2005). Moreover, after 9/11, the focus of researchers and practitioners has shifted from securing the company to ensuring the security of the end-to-end SC (Williams et al. 2008, Donner and Krunk 2009).

Indeed, accidents involving damage, theft, and terrorism have made SC security increasingly more important in the frame of trade globalization. Governments, citizens and companies have different attitudes towards SC security. Governments are concerned about terrorists placing weapons of mass destruction within the country borders e.g. by means of containers moving along the SCs. Citizens and companies – even with various viewpoints – are concerned about the costs of security and the risks of disruptions in case of terroristic attacks (Lee and Whang 2005, Meixell and Nibis 2008). To make SC security more effective, companies and governments should

cooperate both to protect assets security and to prevent the illegal flows of products (Grainger 2007).

By focusing on the flows of goods, 90% of trading is done on a global scale and most of it via containers (Kim et al. 2008): the global container traffic in 2010 was about 115 million of Twenty-foot Equivalent Unit (TEU) containers, soared by more than 10% with respect to 2009. To increase SC security globally, there is no other way than protecting container transport from tampering, theft and other practices leading to place illegal weapons or terrorists in the containers (Sarathy 2005). This is a challenging goal, given the huge number of players involved in the intermodal SCs, particularly when transshipments take place (Cigolini and Rossi 2010, Cigolini *et al.* 2013a, 2013b).

In a typical intermodal SC, there are seven main players. First, the industrial client, who triggers the intermodal transport. Second, the Multimodal Transport Operator (MTO), who arranges the end-to-end intermodal transport. Third, the road carrier, who deals with road transport. Fourth, the intermodal terminal operator, who takes care of reshipping the intermodal loading unit. Fifth, the rail operator, who sorts out the rail transport. Sixth, the railways network manager, who is responsible for managing the rail traffic and for maintenance. Finally, the commercial operator of the rail transport, who plans the rail transport in detail, it is a key player, in that it represents the contact point of MTO, rail operator and rail manager.

According to a vast majority of researchers and practitioners, improvements in SC security are obtained leveraging on two types of sources (Pero and Sudy 2014). First, technology-driven solutions, i.e. sensors, seals and RFiD tags (Lee 2004), used e.g. to keep the doors closed (Rizzo et al. 2010). Second, organizational and cultural tools, i.e. practices implemented to increase SC security by acting on workers and on business partners, through cultural changes (Lee and Whang 2005, Autry and Bobbitt 2008).

Organizational and cultural tools highlight the relevance of the human factor – through values, motivations, attitudes and behaviors – in determining the overall SC security level (Lacey 2010). This distinctive feature attracted the attention of many researchers over the last decade (e.g. Closs and Garrel 2004, Autry and Bobbit 2008, Urcioli 2010). However, a thorough overview of the impacts of cultural and organizational tools on SC security still lacks, particularly within some specific industry. Therefore, this paper aims to study the application of organizational and cultural tools within the intermodal rail and road transport industry, by analyzing some case studies of companies operating in Central Europe, particularly Northern Italy and Switzerland.

The remainder of the paper is organized as follows. Section 2 is devoted to the literature taxonomy on organizational and cultural tools. Then, section 3 introduces the research questions and the logical model, while section 4 outlines the methodology. Finally, section 5 discusses the main results and section 6 draws the conclusions along with some management-related implications and future research paths.

2. Background

Culture is the structure of values shared along the company that helps understand the ways organizations work (Desphande and Webster 1989) and sets the rules for internal behavior (Schein 2010). Many researchers have studied organizational

culture, particularly from the perspective of SC management (Williams et al. 2009). SC security is strongly dependent on the company culture, in that security comes from common and shared values.

In addition, some researchers noticed that culture affects both company's *modus operandi* and relationships with suppliers and customers (Brandolese and Cigolini 1999, Brun and Pero 2011). McAfee et al. (2002) stated that consistency of both internal and external organizational culture is the basis for successful partnerships. SC security orientation (Autry and Bobbitt 2008) and SC security culture (Williams et al. 2009) represent tools to prevent from potential weakness in the SC. According to Lacey (2010), several factors push towards SC security, e.g. the pressure from authorities and private companies, and the awareness that people and companies are both major actors in causing disruptions and key players to restrain adverse consequences.

Finally, Fontaine et al. (2007) observed that an integrated approach (considering both security and safety) leads to cost-efficient protection measures. Other studies suggested that efforts towards security tend to lower total system cost, to improve shipment data and eventually to rise profitability, by preserving market share (Eggers 2004, Sarathy 2006, Williams et al. 2008). Later, through a survey, Williams et al. (2009) highlighted that SC security has an impact on firm's resilience.

Focusing now on culture, Reniers et al. (2011) described security culture by means of people, procedures and technology. These three items apply also to SC security, which depends on the development – within the borders of each node of the SC – of a proper security climate and on the application of tools to diffuse and to increase the security culture. However, when considering SC security culture, you should add SC partners as fourth item: companies are outsourcing activities and they rely on a wide network of suppliers (Pero et al. 2015), thus increasing their dependency on third parties and reducing their ability to control security issues.

Tools involving people encompass tools for selecting, motivating and defining workers' roles and tools for increasing SC security culture within the company (Knight 2003). However, to build the SC security culture, a proactive orientation is needed (Rice and Caniato 2003, Christopher and Peck 2004) and a collaborative attitude between employees and management (Giunipero and Elantawy 2004, Autry and Bobbitt 2008) is advisable.

To prevent breaches, Sheffi (2005) and Reiner and Dullaert (2007) outlined the importance of the detection done by workers: you should train personnel to spot a threat and encourage them to report such issues. Sheffi (2001) early recognized the importance of the role of security manager. Later, Closs and McGarrel (2004) suggested link incentive systems to security performance. Finally, background investigation of potential employees and partners is to be include in workers' selection procedures (Van Oosterhout et al. 2006). Hired people should follow procedures (Reniers et al. 2011) related to managing emergencies, e.g. reports for incidents (Donner and Krunk 2009), to properly storing and transporting goods, e.g. by sealing cargos and inspections (Knight 2003), or to day-by-day routine, e.g. access control and personnel identification (Urcioli 2010).

The technological dimension encompasses all the technology-based tools for sharing information. Procedures are linked to technologies (Urcioli 2010): they support

the implementation of procedures, e.g. databases, data and network protection through firewalls.

Finally, SC partners are to be involved to increase SC security (Ritter et al. 2007). You should leverage contracts and communication exchange (Knight 2003, Sheffi 2005), reduce the suppliers' base (Sheffi 2001), develop collaborative relationships (Rice and Spayard 2005, Caridi et al. 2005, 2006, Cigolini and Rossi 2008) and keep the SC configuration aligned (Cigolini et al. 2011, 2014).

Therefore, SC security tools include a plethora of activities, both inter- and intra-organizational. Yet, there is little insight into the level of adoption of such tools by firms, particularly with reference to the intermodal rail and road industry.

3. Research framework

To analyze SC security from the organizational and cultural viewpoint the Swiss cheese model is introduced (Ren et al. 2008). This model is widely employed in risk analysis and management, including aviation (Young et al. 2005), engineering and healthcare (Reason 2000, Bayley 2004): it likens systems to multiple slices of cheese, stacked side by side.

In the model, organizational defenses against failures are modeled as barriers, represented as slices of cheese. The holes in the slices represent weaknesses in individual parts of the system and are continually varying in size and position across the slices. The system produces failures when a hole in each slice aligns, thus permitting a trajectory of accident opportunity (Reason 2000), so that a hazard passes through holes in all of the slices, leading to a failure.

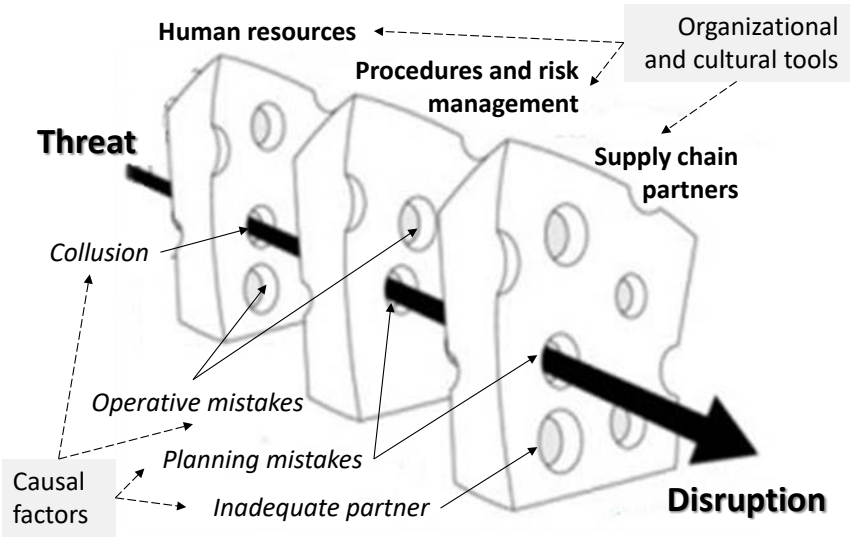

Figure 1. The Swiss cheese model applied to SC security

The main idea behind this work is to use Swiss cheese model to describe the SC security issue (see figure 1). The slices of cheese represent the organization and cultural tools (i.e. human resources, procedures and SC partners) while the holes in the slices

represent the causal factors (collusion, mistakes, errors etc.) reducing SC security. The size of the holes varies, depending on to the tools used and their level of implementation, thus determining the overall SC security performance (i.e. the opportunity for the holes to align): e.g. by increasing company identity (and therefore workers' loyalty) collusion can be mitigated, thus limiting thefts. In the followings, the main elements considered in this work are introduced and described.

3.1. Organizational and cultural tools

To increase SC security both inter and intra-organizational tools can be used. The taxonomy outlined in Table 1 emerges from the literature in the area of SC security culture (i.e. human resources), SC risk management and SC improvement (i.e. SC partners). The area related to the human resources encompasses five tools that aim at developing and spreading SC security culture within a company by acting on people. The second set of tools refers to procedures and risk management tools, which includes procedures and technologies that support the management of companys' vulnerabilities (Jüttner *et al.* 2003). The third set of tools refers to SC partners and it encompasses inter-company tools

3.2. Security performance

Threats affecting SCs are either intentional acts (e.g. thefts, damages, terrorist attacks) or unintentional disruptions (e.g. late suppliers). So security performance can be measured e.g. in terms of stolen (or damaged) containers, whilst unintentional acts might be connected e.g. to a portion of the delayed deliveries to the end customer. In the followings, security against intentional acts are referred as attack security and security against unintentional acts as supply security.

3.3. Causal factors

A disruption can be originated by various causal factors (Bojanc and Jerman-Blazic 2008). According to Arnold (2012), some factors are either intentional and/or connected to company culture (i.e. collusive actions) or even unintentional mistakes, e.g. the lack of employees' consistency to procedures. Other factors are related to wrong procedures planning and to management policies. Finally, some other factors are connected to SC partners, e.g. lack of cooperation and communication between partners, inadequacy of SC partners generated by flaws in procedures and policies.

Area	Tool	Definition	Reference
Human resources	Integrity and loyalty of employees	Tools of employees' selection and affiliation to the company, e.g. investigation on past work experiences, loyalty programs	Sheffi 2001, Sudy 2011
	Internal awareness of security	Tools to diffuse and communicate to the organization the importance of SC security, e.g. training, journals, internal communication on procedures and risks	Closs & McGarrel 2004, Guiterrez & Hitsa 2006
	Shared values	Tools to diffuse the company's values among employees, e.g. company's motto, vision	Lacey 2009
	Cooperation	Tools to increase employees collaboration and cooperation, e.g. team working	Schein 1992
	Roles and responsibilities	Tools to increase company's resilience by leveraging on employees' flexibility, e.g. multitasking workforce	Rice & Caniato 2003, Sudy 2011
Procedures and risk management	Business continuity planning	Tools to increase company's ability to recover from disruptions, e.g. contingency plans, recovery procedures	Autry & Bobbitt 2008
	Incidents and weakness assessment	Tools to assess company's weak points and develop new procedures, e.g. analysis of incidents, weaknesses identification	Wu et al. 2011, Sudy 2011
	Continuous improvement	Tools to support operative process monitoring and improvements, e.g. security managers, collection of ideas on security improvements	Rice & Caniato 2003; Pero & Sudy 2014
	Knowledge management	Tools to gather and diffuse the knowledge about security, e.g. knowledge management systems	Rice & Caniato 2003
	Security procedures	Tools to define procedures and assess company's compliance with existing ones, e.g. certification	Schein 2010, Sudy 2011
Supply Chain partners	SC awareness of security	Tools to assure that SC partners comply with the security levels required by the company, e.g. training, contracts with specific clauses on security	Closs & McGarrel 2004, Williams et al. 2008
	Shared values at SC level	Tools to diffuse the company's values among SC partners, e.g. cultural adaption, mission alignment	Williams et al. 2008, Sudy 2011
	Customer centric SC	Tools to develop a customer driven SC, e.g. collaboration at SC level for SC design	Closs & McGarrel 2004
	Partnership	Tools to develop long term commitment to security of the partners along the SC, e.g. long term contracts, trust	Brun & Pero 2011, Giunipero & Eltantawy 2004

Table 1. Taxonomy of organizational and cultural tools

3.4. Environmental variables

The way SC security is approached depends on some environmental variables, e.g. the SC geographical spread (Whipple et al. 2009). Similarly, environmental variables are expected to affect the effectiveness of organizational and cultural tools. These variables refer to company size, area where the company operates (road, rail, both), company's role within the SC (MTO, road transport, terminal manager, commercial operator), vertical integration and type of transported goods (dangerous, desirable, other goods). Dangerous goods are subject to terroristic and criminal attack, while desirable goods are subject to theft and contamination.

Vertical integration has been measured by considering as highly integrated either companies both in rail and road or companies playing two (or more) roles in one area (i.e. road or rail).

3.5. Research questions

This research aims to investigate the organizational and cultural tools used by companies within the intermodal rail and road industry, to assess the impact of such tools on security-related performance and to analyze the context variables that affect the application of the tools above. Therefore, the following research questions have been developed.

RQ1	What organizational and cultural tools do companies use within the intermodal rail and road industry?
RQ2	How do organizational and cultural tools influence security performance?
RQ3	How do environmental factors affect the use of organizational and cultural tools?

RQ1 aims to provide a picture of how organizational and cultural tools are spread among companies within the intermodal road and rail industry. RQ2 is devoted to investigate whether and how organizational and cultural tools are actually useful to increase SC security. Finally, RQ3 casts light on some environments where organizational and cultural tools are likely to be very more effective. The intermodal and rail and road industry has been selected mainly due to the lack of studies in this field.

3.6. Methodology

Since SC security-related problems seemed too ill structured to allow a simulation-based approach (Cigolini et al. 2011, 2014, 2015), a case-based methodology has been chosen. Case studies are a powerful approach to understand complex phenomena, and whenever there is the need to answer to *how* and *why* questions (Yin 2003). Moreover, case studies appeared appropriate given the attempt – made here – to validate findings through cross-case comparisons (Eisenhardt 1989).

Table 2 shows the sample. All the companies are located in Italy or in Switzerland and they operate in the intermodal road and rail transport industry. To balance the need for a large sample and the need for an in-depth analysis of each case, 13 companies have been selected, based on their explicit interest in SC security.

Company	Employees	Sales (Mln €)	Area of expertise	Integration level	Internationalisation	Role of the company in the SC	Transported goods
A	249	80	Road	High	Int. nal	Multimodal & road Transport and Terminal Manager & Commercial operator	Desirable
B	210	29	Road	Low	Int. nal	Multimodal & road transport operator	Desirable & dangerous
C	1,600	395	Road	Low	Int. nal	Multimodal transport operator	Desirable & dangerous
D	1,854	430	Road	Low	Int. nal	Multimodal transport operator	Desirable & dangerous
E	5,200	990	Road	Low	Int. nal	Multimodal & road transport operator	Dangerous
F	401	365.4	Rail	High	Int. nal	Terminal manager and Commercial operator	Desirable & dangerous
G	600	52	Road & rail	High	Int. nal	Multimodal transport operator and Terminal manager	Desirable & dangerous
H	90	13.5	Road	Low	Int. nal	Multimodal transport operator & road transport	Dangerous
I	36	11	Road & rail	High	Int. nal	Multimodal transport operator &Terminal manager	Others
J	150	56	Road & rail	High	Int. nal	Multimodal & road transport operator and Terminal manager	Desirable & dangerous
K	202	16.5	Rail	Low	Local (Italy)	Terminal manager	Desirable & dangerous
L	8	0.4	Rail	Low	Local (Italy)	Terminal manager	Desirable & dangerous
M	107	144.5	Road	High	Int. nal	Multimodal transport and Commercial operator	Dangerous

Table 2. The sample of the analyzed companies

Secondary sources have been analyzed to find companies (i) claiming that security is a competitive priority or (ii) highlighting they have performed actions to increase employees' awareness on security, or even (iii) managing high-value goods, which requires security to be carefully managed. Indeed, companies have been selected using a twofold approach (Yin 1984). First, the literal replication approach (to get convergent results) which led e.g. to companies playing the same role in the SC and managing similar products. Second, the theoretical replication approach (to explore different SC security practices), which led e.g. to various actors (road carrier, intermodal terminal etc.) belonging to the intermodal SC to be represented in the sample.

Information has been gathered through direct semi-structured interviews (see Appendix 1) with senior managers, previously informed that data provided would be useful to prepare a high-standard final report, to be shared among participants only. The interviews have been conducted mainly with Chief Operating Officers (COOs) and sometimes with Accounting Managers, General Managers, Chief Executive Officers (CEOs), and Sales Directors. On average, each manager has been interviewed two times, devoting three hours per interview. All interviews have been tape-recorded and transcribed. Usually, a telephone follow-up with the respondents was conducted to assess the outcomes and – if needed – to gather missing data.

Before each interview, secondary information (company reports, procedures etc., e.g. about the number of thefts) was collected and compared with data drawn from the interviews, to ensure construct validity (Yin 1984). Information gathered through interviews and secondary sources has been categorized and contextualized (see e.g. Miles and Huberman 1984), to reveal unexpected relationships between events and circumstances. These structured procedures for data collection and analysis, and the use of the semi-structured interview guide, helped enhance the research reliability (Yin 1984).

Table 3 summarizes the main results regarding the tools used by the companies of the sample and the tools rated as very important to increase security. Human resources-related tools are not applicable to MTOs, since they do not have direct employees, whereas 'partnership' is not applicable to the newborn company L.

4. Results

This section presents the main results coming from the analysis of the case studies, according to the research questions stated in section 3.5.

4.1. Results about RQ1

Figure 2 shows the use and the importance of each tool as perceived by companies. The importance of each tool has been calculated as the ratio between the number of companies considering the corresponding tool as "highly important" and the number of cases where the tool is applicable.

Main area		A		B		C		D		E		F		G		H		I		J		K		L		M	
		Use	Importance	Use	Importance	Use	Importance	Use	Importance	Use	Importance	Use	Importance	Use	Importance	Use	Importance	Use	Importance	Use	Importance	Use	Importance	Use	Importance	Use	Importance
Human resources	Integrity and loyalty of employees	Y	HI	Y		N	NA	N	NA	Y		Y	HI	Y	HI	Y		N		Y	HI	Y		N		Y	NA
	Internal awareness of security	Y		Y	HI	N	NA	N	NA	Y	HI	Y	HI	Y	HI	Y	HI	Y		Y		N		Y		Y	NA
	Shared values	N		Y		Y	NA	Y	NA	Y		Y		Y		Y		N		Y		N		Y		Y	NA
	Cooperation	Y	HI	Y	HI	N	NA	N	NA	Y		Y	HI	Y	HI	Y	HI	Y	HI	Y	HI	Y	HI	Y	HI	N	NA
	Roles and responsibilities	Y		N		N		N		Y		Y		Y	HI	N		Y	HI	Y		Y		N		N	
Procedures and risk management	Business continuity planning	N		N.		N		N.		N		Y		Y		N		N		N		N		N		Y	
	Incidents and weakness assessment	Y		Y	HI	Y	HI	Y		Y	HI	Y	HI	N		Y	HI	Y	HI	Y		Y	HI	Y	HI	N	HI
	Continuous improvement	N	HI	Y		Y		Y		Y		Y		Y	HI	Y		Y		Y		Y	HI	N		Y	HI
	Knowledge management	N		N		N		N		Y	HI	N		N		N		N		N		N		N		Y	
	Security procedures	Y		Y	HI	Y	HI	Y	HI	Y	HI	Y		Y		Y		Y		Y		Y		Y		Y	HI
Supply Chain partners	Supply chain awareness of security	Y	HI	N		Y		Y		Y	HI	Y		Y		Y		Y		N		Y		N		Y	HI
	Shared values at supply chain level	Y		N		Y		Y		Y		Y		N		Y		Y		N		Y		N		Y	
	Customer centric supply chain	Y	HI	N		Y		Y		N		N		N		N		N		N		N		N		Y	
	Partnership	Y		Y		Y		Y		Y		Y		Y		Y	HI	Y	HI	Y		N		Y	NA	Y	

Legend: NA = Not Applicable; HI = Highly Important; Y = yes; N = no;

Table 3. Tools used by the companies and tools rated as “highly important” (HI) through the interviewed companies

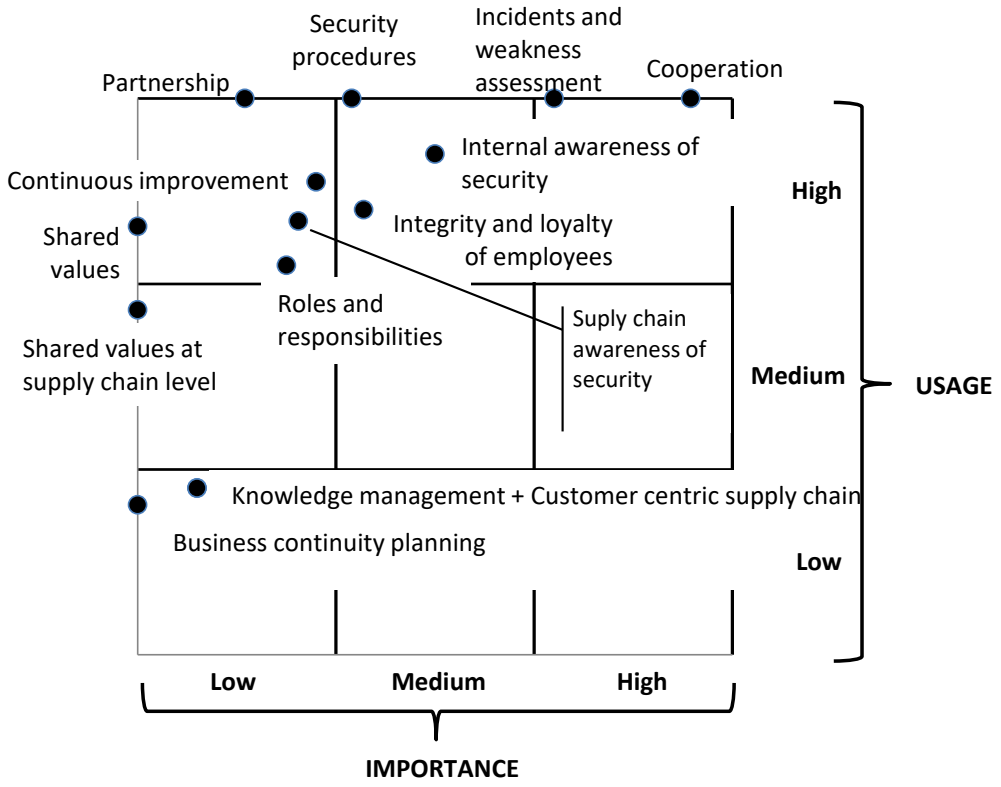

Figure 2. Usage vs. importance of organizational and cultural tools.

Even at first sight, the majority of tools appear highly used. Since within the intermodal industry the human factor is very relevant, all the interviewed companies believe that human resources and procedures are important to increase security. Therefore, the tools both widely used and perceived as important are: cooperation, internal awareness of security, integrity and loyalty of employees, security procedures, and incidents and weaknesses assessment.

Three tools are in the bottom-left corner (low usage, low importance): business continuity planning is not popular, since it is hard to implement in the intermodal sector, due to the huge number of variables to be taken into account. Moreover, many interviewees pointed out that relevant portions of the intermodal SC depend on actors that are out of company's control (e.g. the railway infrastructure), so that business continuity planning is not widespread. Knowledge management is easy to implement in knowledge-intensive industries, so most of the interviewed companies rely on informal tools, such as employees training. Finally, customer centric SC is not used because the intermodal industry is very fragmented. Besides, an incentive system that could guarantee specific attention to good results in the field of security within all the layers of the SC is still lacking.

Some tools, even widely used, appear irrelevant to enhance security (roles and responsibilities, shared values, continuous improvement, partnership and shared values at SC level): they are used with a purpose different from security, e.g. to speed-up

quality management programs or to troubleshoot logistics processes. A conspicuous example is in partnerships, developed to reduce delivery lead times, by improving shipment planning (company C), by reducing suppliers' selection time (company D and F), or by increasing communication (company H) and visibility through tracking and tracing systems (company I). SC awareness of security seems to be ineffective due to the lack of trust in SC partners' capabilities.

To summarize, results about RQ1 suggest that companies within the intermodal rail and road industry, mainly rely on internal procedures and human resources management tools to tackle SC security issues. External partners are not perceived as trustworthy enough to ensure SC security.

4.2. Results about RQ2

The contribution of cultural tools on both attack security and supply security has been assessed based on respondents' answers.

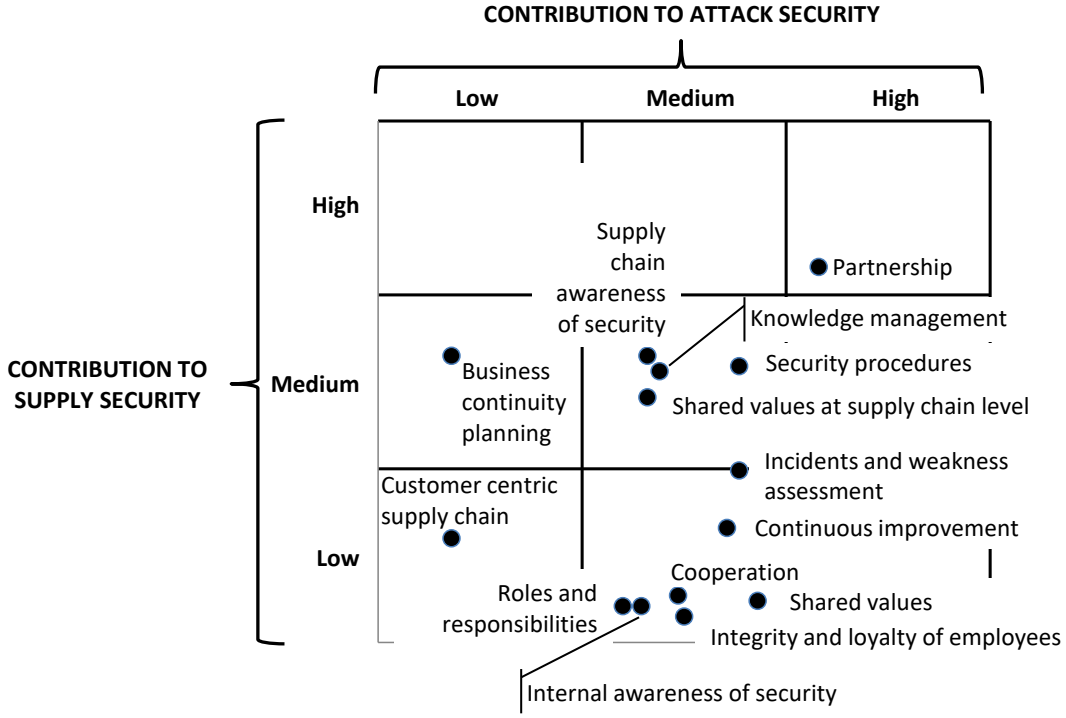

Figure 3. Contribution of various organizational and cultural tools to increase security

Figure 3 shows that attack security can be improved by internal and external tools, while supply security can be tackled mainly by involving SC partners: tools involving human resources are considered capable to reduce the number of thefts, but with limited impact on supply security. Partnership is the most important tool, in that it influences both type of security. This does not match with the importance vs. usage matrix (see figure 2) where companies consider partnership as a low-importance tool. Indeed, partnerships are often developed to increase operative performance, such as

visibility, which is considered an important performance index within the intermodal rail and road industry, at the expenses of SC security. So, despite the recognized potential to improve security, the use of partnership for security improvement still lacks. On the other hand, a customer centric SC is considered as a low-impact tool, in line with the results of the analysis developed above.

Table 4 casts light on the contribution of the different tools to increase security, by linking the tools to the causal factors that lead to low security performance. Each cell contains the cases where a positive (+), negative (-) or both positive and negative (+/-) impact on security performance has been found. Below each causal factor, the companies of the sample that indicated the corresponding causal factor as important in determining security performance are listed.

As far as the attack security, tools related to human resources are widely considered as the main instruments to reduce operative mistakes. Besides, tools related to procedures and risk management play a major role in reducing the number of thefts due to operative and planning mistakes. The sole exception is the business continuity planning, since it encompasses recovery plans after an accident has occurred. Within the intermodal rail and road industry, truck drivers are responsible for the implementation of procedures, therefore, attack security significantly depend on their awareness of procedures.

Within SC-related tools, partnership is able to reduce thefts, by acting on all causal factors. Partnerships guarantee that partners are following predefined procedures and reduce collusion (company G) and that have an integrated information system to reduce operative mistakes (company K).

As far as supply security, in line with the results about attack security, operative mistakes can be sorted out through tools related to human resources. Planning mistakes can be sorted out through tools related to procedures and risk management. The lack of cooperation and/or communication between partners is addressed by developing partnerships and a customer centric SC. However, a general agreement on a set of tools able to reduce the adverse impact of an inadequate partner has not been reached.

As far as the importance of causal factors in determining security performance, different results have been found for attack security and supply security. Indeed, according to all the respondents, attack security performance is determined by three main causal factors, i.e. collusion, operative mistakes and planning mistakes. Besides, supply security depends on the lack of cooperation and/or communication between partners, on inadequate partners and on operative and planning mistakes.

The majority of respondents stated that an inadequate partner mostly determines supply security: the lack of cooperation and/or communication between partners mitigates or amplifies the effect (on supply security) of an inadequate partner. Consistently, respondents feel that organizational and cultural tools do not have a strong impact on this causal factor. Moreover, the majority of small companies does not perceive collusion as relevant, whereas large companies highlight it as a major issue.

Main area	Tool	Attack security			Supply security			
		Collusion	**Operative mistakes**	**Planning mistakes**	**Lack of cooperation …**	**Inadequate partner**	**Operative mistakes**	**Planning mistakes**
		A;C;D;G	*F;G;K;L*	*B;E;J;M*	*A;B;J*	*ALL*	*G*	*M*
Human resources	Integrity and loyalty of employees	+ (A; E; F; J; K)	+ (B; E; G; J; K)				+ (B; E; G; H; J; K)	
	Internal awareness of security	+ (B; E)	+ (A; B; E; F; G; J; L)	+ (A)			+ (A; E; F; G; H; I; J; L)	+ (A; H);
	Shared values	+ (B; C; E; F; G; J; M)	+ (B; C; D; E; F; G; J; M)	+ (F; J)	+ (C)		+ (B; C; E; F; H; J; M)	+ (F; J)
	Cooperation	+/- (A) + (G; K)	+ (A; B; E; F; G; J; K; L)	+ (A)	+(A)		+ (A; B; E; F; G; H; I; J; K; L)	+ (A)
	Roles and responsibilities	- (A, L)	+ (A; E; F; G; J; K)	+ (A)			+ (A; E; F; G; I; J; K)	+ (A)
Procedures and risk management	Business continuity planning			+ (G)		+ (M)	+ (F)	+ (G; M)
	Incidents and weakness assessment	+ (M)	+ (A; B; E; F; G; K; M)	+ (A; B; C; D; E; F; G; J; K; M)	+ (E)	+ (E; H; I; M)	+ (A; B; E; F; G; I; K; L; M)	+ (A; B; C; D; E; F; G; H; I; J; K; M)
	Continuous improvement		+ (B; E; F; J; K)	+ (B; C; D; E; F; G; J; K; M)		+ (E; M)	+ (B; E; F; I; J; K;	+ (B; C; D; E; F; G; H; I; J; K; M)
	Knowledge management	+/- (G)	+ (E; G)	+ (D; E; M)	+ (E; M)	+ (E; M)	+ (E; G)	+ (D; E; M)
	Security procedures	+ (C; D; F; J)	+ (A; C; D; E; J; L)	+ (A; B; D, E; F; G; J; L; M)	+ (J)	+ (B; D; E; H; I; J; M)	+ (A; C; D; E; H; I; J; K; L)	+ (A; B; D; E; F; G; H; I; J; L; M)
Supply chain partners	SC awareness of security	+ (A; M)	+ (A; D; E; F; G)	+ (D; E; M)		+ (A; C; D; E; H; I; K; M)	+ (A; D; E; F; G; H; I)	+ (D; E; H; M)
	Shared values at SC level	+ (A; C; M)	+(C; D; E)	+ (A; F)	+ (F; I; M)	+(A; E; F; M)	+ (C; D; E; H)	+ (A; F; H)
	Customer centric SC	- (A)	+(C)	+ (D)	+(A; C; M)		+ (C; M)	+ (D; M)
	Partnership	+ (A; D; E; F; G; J; M)	+ (A; E; F; G; J)	+ (A; B; D; E; F; G; J; M)	+ (A; B; D; E; F; G; H; I; J; L; M)	+ (A; D; E; F; G; H; J; M)	+ (A; E; F; G; H; I; J; L)	+ (A; B; D; E; F; G; J; M)

Table 4. Impact on causal factors determining attack and supply security

To summarize, with reference to RQ2, operative and planning mistakes are important factors to determine both attack and supply security. Collusion is a relevant causal factor of attack security, whereas the lack of cooperation and/or communication between partners, together with inadequate partners are key factors to reduce supply security.

4.3. Results about RQ3

Three environmental factors proved to be able to affect the adoption of organizational and cultural tools: company size, level of vertical integration and area of activity. Referring to company size, the bigger the company, the more the tools are standardized and formalized: the internal complexity prevents from achieving security target without a formal use of the tools. Besides, both in large and small companies, roles and responsibilities, incidents and weaknesses assessment, security procedures and partnership are very popular. No small company uses customer centric SC, knowledge management and business continuity planning.

In terms of importance, partnership is significant for small companies, while large companies do not use it at all. Small companies leverage the good and long-lasting relationships with suppliers to gather information on disruptions and thefts, to increase the service level and to trigger continuous improvement. Regarding the integration, there is no clear difference in the use of the proposed tools. Integration is a discriminant factor only for two tools, i.e. roles and responsibilities (although it is better explained by the area of work, i.e. whether rail or road is involved) and business continuity planning. The benefits of using the latter tool depend on the availability of alternative rail routes.

Considering contingency factors (i.e. rail or road or both), a difference can be spotted between the use and the importance given by companies to roles and responsibilities, and shared values at SC level. Companies operating only or also in the rail area tend to rely on multi-tasking workforce: this depends on the huge number of activities to perform in a terminal with respect to road companies. This triggers the need to reduce labor specialization for the sake of flexibility (see companies A, J, L), and to spread process knowledge to increase customer orientation and to solve problems quicker (companies F, G, I).

The companies operating on road use the shared values at SC level. They are interested in making their partners share a common view on SC security (company C) or they are trained on security issues (company E), since they are closer to the final customer and thus responsible of shipping delays and troubles. Road companies pay more attention than terminal operators and rail operators to the internal awareness of security. This can be due to the reduced number of variables that can generate a disruption in a terminal with respect to a road.

To summarize, both company size and company area of business affect the tools used to increase SC security. Large companies rely more on formalized tools, whereas small companies tend to trust SC partners. Companies operating on road are more oriented to develop a SC security consciousness (at company and at SC level) than companies operating in the rail industry are.

4.4. Summary of results and managerial implications

To face SC security challenges, the companies of the sample strongly rely on their internal resources (procedures and people). To increase SC security, they have not exploited yet the potential of the tools traditionally used to collaborate along the SC (i.e. partnership), despite they know those tools very well. Since partnerships are already in place with suppliers, not to leverage the already used tools also to increase SC security appears to be a loss of opportunity for companies.

To help managers define a set of tools to manage both attack and supply security, a checklist – based on table 4 – has been developed (see table 5). A given tool (marked with an X) has been considered as relevant to reduce the adverse impact of a considered causal factor whenever more than 50% of the companies in the sample stated that they used it. In this way, managers can use table 5 either to check whether each tool is useful to reduce the adverse impact of each causal factor or they can evaluate the opportunity to implement such a tool, by predicting the impact on the causal factors.

		Attack security			Supply security			
Main area	**Tool**	Collusion	Operative mistakes	Planning mistakes	Lack of cooperation / communication between partners	Inadequate partner	Operative mistakes	Planning mistakes
Human resources	Integrity and loyalty of employees							
	Internal awareness of security		X					
	Shared values	X	X				X	
	Cooperation		X				X	
	Roles and responsibilities						X	
Procedures and risk management	Business continuity planning						X	
	Incidents and weakness assessment		X	X				
	Continuous improvement			X			X	X
	Knowledge management							X
	Security procedures			X				
Supply chain partners	SC awareness of security						X	X
	Shared values at SC level					X	X	
	Customer centric SC							
	Partnership	X		X	X	X	X	X

Table 5. SC security tools checklist

With respect to the adverse impact of an inadequate partner on SC security, results suggest that a general agreement on a set of tools able to reduce it has not been reached yet. Three main approaches have been observed. Company E and M follow a 'multilateral' approach, in that they leverage on practices other than partnership, ranging from internal procedures to continuous improvement. 'Pessimistic' companies

(e.g. B, C, G, K, L) see the inadequate partner as an unavoidable problem, so they do not use at all or use just one tool to manage inadequate partners. Finally, 'focused' companies (e.g. A, D, F, H, I, J) pinpointed several tools to mitigate partner inadequacy, and they take advantage on practices at SC level. Unfortunately, quantitative data is not available to test the effectiveness of different strategies to improve security performance: future developments are going to cover this issue.

5. Concluding remarks and future research paths

This research study investigates the adoption of organizational and cultural tools to increase SC security performance within the intermodal road-and-rail industry. In particular, using the Swiss cheese model as standpoint, it investigates: (i) the used tools within the industry; (ii) how the tools used affect security performance; (iii) what environmental factors determine the adoption of each tool.

Results suggest that organizational and cultural tools positively affect SC security performance, by reducing the collusion and operative and planning mistakes, which are the cause of manipulation and theft. Besides, such tools mitigate the problems connected to the lack of cooperation and communication between partners and to inadequate partners, which are the cause of delays in the delivery of goods to the final customers.

All the companies of the sample recognize the benefits of organizational and cultural tools. However, results clearly indicate that the ability of tools to increase SC security has not been fully exploited yet: quite a number of companies report that most of the considered tools – almost as they are used now – are unable to remarkably improve the overall SC security performance. Moreover, despite an inadequate partner has been found as the most relevant causal factor in determining delayed deliveries to end customers, the corresponding organizational and cultural tools are not used enough or they are not considered powerful enough to mitigate that factor. Besides, the level of adoption of the various organizational and cultural tools has proved significantly different depending on company size, area of activity and vertical integration.

Finally, this study has clearly outlined many promising future research paths in the field of SC security. These paths can be grouped in three major areas, briefly outlined hereinafter.

The first area relates to the opportunity of broadening the research borders: the case-based approach employed here can be successfully applied to industries other than rail and road or to countries other than Italy and Switzerland, both in Europe and abroad. This way of doing might lead to confirm and extend some of the results presented in this study.

The second area relates to the opportunity to strengthen the research framework. The way this be accomplished is almost threefold: (i) by enriching and improving the list of organizational and cultural tools, (ii) by improving the list of performance measures and (iii) by better structuring a list of causal factors. Based on this standpoint, a cause-effect diagram could be outlined, to assess the expected impact of each tool on each factor and performance.

The third area consists in applying a very different methodological pattern: instead of a few case studies analyzed in depth, a mathematical model, possibly coupled

with simulation, could be developed based on the early results highlighted here. Besides and possibly again in conjunction with simulation, an extensive survey can be carried out, to support via statistical analyses the results of the present study.

Appendix 1

All the interviews have been carried out by means of the following semi-structured questionnaire.

1. Company and company culture:
    - Role of the company in the SC, activities and services, revenues, employees, main clients / customers, organization, transported goods.
    - Company history, vision and mission
2. Security management:
    - Organizational tools used to manage SC security
    - Tools' implementation (e.g. formalized /not, company / SC level etc.); examples of tools and applications.
    - Rating the importance of tools listed in Table 1; motivation for their importance (or not) with reference to the company
3. Security performance measurement
    - Impact of the proposed tools to help reduce the number of thefts
    - How the proposed tools succeeded in reducing thefts
    - Impact of the tools proposed to help reduce the effect of unintentional threats
    - How the proposed tools succeeded in reducing unintentional thefts
    - Impact of the causal factors in determining the security performance
    - List of other factors that are likely to determine the security performance
    - Contribution of each tool in Table 1 to reduce the adverse effect of each causal factor on security performance

References

Arnold, U. Neubauer, J., Schoenherr, T. (2012), "Explicating factors for companies' inclination towards corruption in operations and SC management: an exploratory study in Germany", International Journal of Production Economics, 138 (1), 136-147.

Autry, C.W., Bobbitt, L.M. (2008), "Supply chain security orientation: conceptual development and a proposed framework", The International Journal of Logistics Management, 19 (1), 42-64.

Bakshi, N., Gans, N. (2010), "Securing the containerized supply chain: analysis of government incentives for private investment", Journal of Management Science, 56 (2), 219-233.

Bojanc, R., Jerman-Blazic, B. (2008), "An economic modelling approach to information security risk management", International Journal of Information Management, 28 (5), 413-422.

Bayley, C. (2004). "What medical errors can tell us about management mistakes" In: Hofmann, P.B., Perry, F. "Management mistakes in healthcare: identification, correction, and prevention". Cambridge University Press. (ISBN 0521829003).

Brandolese, A., Cigolini, R. (1999) "A new model for the strategic management of inventories subject to peaks in market demand", International Journal of Production Research, 37 (8), 1859-1880.

Brun, A., Pero, M. (2011), "Assessing suppliers for strategic integration: a portfolio approach", International Journal of Business Excellence, 4 (3), 346-370.

Caridi, M., Cigolini, R., De Marco, D. (2005) "Improving supply chain collaboration by linking intelligent agents to CPFR", International Journal of Production Research, 43 (20) 4191-4218.

Caridi, M., Cigolini, R., De Marco, D. (2006) "Linking autonomous agents to CPFR to improve SCM", Journal of Enterprise Information Management, 19 (5), 465-482.

Christopher, M., Peck, H. (2004), "Building the resilient supply chain", International Journal of Logistics Management, 15 (2), 1-14.

Cigolini, R., Pero, M., Rossi, T. (2011) "An object-oriented simulation meta-model to analyze supply chain performance", International Journal of Production Research, 49 (19), 5917-5941.

Cigolini, R., Pero, M., Rossi, T. (2013a), "Sizing off-shore transshipment systems: a case study in maritime dry-bulk transportation", Production Planning and Control, 24 (1), 15-27.

Cigolini, R., Pero, M., Rossi, T., Sianesi, A. (2015) "Using simulation to manage project supply chain in the off-shore oil and gas industry", Production Planning and Control, Vol. 26, No. 3, pp. 167–177.

Cigolini, R., Pero, M., Rossi, T., Sianesi, A. (2014) "Linking supply chain configuration to supply chain performance: a discrete event simulation model", Simulation Modelling Practice and Theory, 40, 1-11.

Cigolini R., Pero, M., Rossi, T., Sianesi A. (2013b) "Using simulation to optimize transshipment systems: Applications in field", Maritime Economics and Logistics, 15 (3), 332–348.

Cigolini, R., Rossi, T. (2008) "Evaluating supply chain integration: a case study using fuzzy logic", Production Planning and Control, 19 (3), 242-255.

Cigolini, R., Rossi, T. (2010) "Sizing off-shore transshipment systems in dry-bulk transportation", Production Planning and Control, 21 (5), 508–522

Closs D.J., McGarrel E.F. (2004), "Enhancing security throughout the supply chain", Special report series of IBM Centre for the business of Government.

Desphande R., Webster F.E. (1989), "Organizational culture and marketing: defining the research agenda", Journal of Marketing, 6 (2), 204-223.

Donner M., Kruk C. (2009), "Supply chain security guide", The World Bank, Washington.

Eggers, W.D. (2004), “Prospering in the secure economy”, Internal publication of Deloitte Touche Tohmatsu, New York, NY, available at: www.deloitte.com

Eisenhardt, K. (1989), “Building theories from case study research”, The Academy of Management Review, 14 (4), 532-550.

Fontaine F., Debray, B., Salvi O. (2007), “Protection of hazardous installations and critical infrastructures: complementarity of safety and security approaches. In: Linkov, I., et al. (Editors), Managing Critical Infrastructure Risks. Springer, London, 65-78.

Grainger A. (2007), “Supply chain security: adding to a complex operational and institutional environment”, World Customs Journal, 1 (2), 25-37.

Giunipero, L.C., Eltantawy, R.A. (2004), “Securing the upstream supply chain: a risk management approach”, International Journal of Physical Distribution and Logistics Management, 34 (9), 698-713.

Jüttner, U., Peck, H., Christopher, M. (2003), “Supply chain risk management: outlining an agenda for future research”, International Journal of Logistics Research and Applications, 6 (4), 197-210.

Kim, S.J., Deng, G., Gupta, E. (2008), “Enhancing cargo container security during transportation: a mesh networking based approach”, Proceedings of the 2008 IEEE International Conference on Technologies for Homeland Security, May 12th – 13th, Waltham, MA Greater Boston.

Knight P. (2003), “Supply chain security guidelines”, White Paper, IBM, available at: www.ibm.com

Lacey D. (2009), “Managing the human factor in information security”, Wiley, London, UK.

Lacey D. (2010) “Understanding and transforming organizational security culture”, Information Management and Computer Security, 18 (1), 4-13.

Lee H.L., Whang S. (2005), “Higher supply chain security with lower cost: lessons from total quality management”, International Journal of Production Economics, 96 (3) 289-300.

Matsika E., Ricci S., Mortimer P., Georgiev N., O’Neill C. (2013) “Rail vehicles, environment, safety and security”, Research in Transportation Economics, 41, 43-58.

McAfee, R.B., Glassman, M., Honeycutt, E.D. Jr (2002), “The effects of culture and human resource management policies on supply chain management”, Journal of Business Logistics, 23 (1), 1-18.

Meixell, M. J., Norbis, M. (2008), "A review of the transportation mode choice and carrier selection literature", The International Journal of Logistics Management, 19 (2), 183–211.

Miles, M.B., Huberman, A.M. (1984), “Qualitative Data Analysis”, Newbury Park, Sage.

Pero, M., Sudy, I. (2014), “Increasing security and efficiency in supply chains: a five-step approach”, International Journal of Shipping and Transport Logistics, 6 (3), 257-279

Pero, M., Stößlein, M., Cigolini, R. (2015) Linking product modularity to supply chain integration in the construction and shipbuilding industries, International Journal of Production Economics (available on line) http://www.sciencedirect.com/science/article/pii/S0925527315001632 ; DOI:10.1016/j.ijpe.2015.05.011

Reason, J. (2000). “Human error: models and management”. British Medical Journal, 320, 768–770.

Ren, J., Jenkinson, I., Wang, J., Yang, J.B. (2008) “A methodology to model causal relationships on offshore safety assessment focusing on human and organizational factors”, Journal of Safety Research, 39 (1), 87–100.

Reniers, G.L.L., Dullaert, W. (2007), “Gaining and Sustaining Site-integrated Safety and Security in Chemical Clusters”, Nautilus Academic Books, Zelzate, Belgium.

Reniers, G.L.L., Cremer, K., Buytaert, J. (2011), “Continuously and simultaneously optimizing an organization's safety and security culture and climate: the Improvement Diamond for

Excellence Achievement and Leadership in Safety and Security (IDEAL S&S) model", Journal of Cleaner Production, 19 (11), 1239-1249.

Rice J.B., Caniato F. (2003), "Building a secure and resilient supply chain", Supply Chain Management Review, Sept./Oct., 22-33.

Rice, J.B. Jr., Spayd, P.W. (2005), "Investing in supply chain security: collateral benefits", IBM Centre for The Business of Government. Special Report Series.

Ritter, L.J., Barrett, J., Wilson, R. (2007), "Securing Global Transportation Networks: A Total Security Management Approach", McGraw Hill, NY.

Rizzo F., Barboni, M., Faggion, L., Azzalin, G., Sironi, M. (2011), "Improved security for commercial container transports using an innovative active RFID system", Journal of Network and Computer Applications, 34, 846-852.

Sarathy R. (2006), "Security and the global supply chain", Transportation Journal, 54 (4), 21-28.

Sheffi Y. (2001) "Supply chain management under the threat of international terrorism", International Journal of Logistics Management, 12 (2), 1-11.

Sheffi Y. (2005), "The resilient enterprise: overcoming vulnerabilities for competitive advantage", The MIT Press, Cambridge, MA.

Schein, E.H. (2010), "Organizational culture and leadership", Jossey-Bass, San Francisco, USA.

Sudy, I. (2011) "Improve the supply chain for container transport and integrated security simultaneously", unpublished deliverable document 6.1 of the IMCOSEC project, contract: SEC-242295

Urciuoli L. (2010), "Supply chain security-mitigation measures and a logistics multi-layered framework", Journal Transport Security, 3 (1), 1-28.

Van Oosterhout M., Veenstra A.W., Mejjer M.A.G., Popal, N., Van Der Berg, J. (2007), "Visibility platforms for enhancing supply chain security: a case study in the port of Rotterdam", Proceedings of the international symposium on maritime safety, security and environmental protection, Athens (Greece), 20th - 21th September.

Veenstra A.W. (2005), "Supply chain security Definitions, PROTECT report D1.2", RSM Erasmus University Rotterdam.

Whipple, J.M., Voss, M.D., Closs, D.J. (2009), "Supply chain security practices in the food industry: do firms operating globally and domestically differ?", International Journal of Physical Distribution and Logistics Management, 39 (7), 574-594.

Williams, Z., Lueg, J.E., LeMay, S.A. (2008), "Supply chain security: an overview and research agenda", The International Journal of Logistics Management, 19 (2), 254-281.

Williams Z., Ponder, N., Autry, C.W. (2009), "Supply chain security culture: measure development and validation", The International Journal of Logistics Management, 20 (2) 243-260.

Yin K.R. (1984) "Case study research. Design and methods", Sage Publications.

Young, M.S., Shorrock, S.T., Faulkner, J.P.E (2005). "Seeking and finding organizational accident causes: comments on the Swiss cheese model". Internal report of the Department of Aviation, University of New South Wales.